AMENDMENT TO THE CLAIMS

2. (Previously amended) The system of claim 6, wherein the communications engine uses SSL to create a secure communications link with the client.

3. (Previously amended) The system of claim 6, wherein the communications engine negotiates an encryption protocol for transferring messages to and from the client.

4. (Previously amended) The system of claim 6, wherein the communications engine uses public key certificates for transferring messages to and from the client.

5. (Currently amended) The system of claim 6, wherein the security services use public key certificates to authenticate a user of the client to determine the user ~~client~~ privileges.

6. (Currently amended) A system on a server computer system, comprising:

a communications engine for establishing a communications link with a client;

security services coupled to the communications engine for presenting to a user of the client a plurality of user authentication protocol options, each user authentication protocol option having a particular level of authentication associated with it, for authenticating the user according to at least one user authentication protocol and for determining ~~client~~ user privileges based on ~~, the security services further capable to examine~~ the identity of ~~a~~ the user ~~of the client~~ and the level of authentication ~~to determine the client privileges~~;

a web server for presenting a set of available services based on the user privileges, at least one of the available services requiring additional authentication information to be provided before access to the service is granted, and for enabling the client to select a particular service from ~~a~~ the set of available ~~personal information management~~ services~~,~~ ~~the set of available services based on the client privileges~~;

a host engine coupled to the security services and to the web server for providing to the client service communication code that enables communication with the particular ~~a selected~~ service; and

a keysafe for storing keys, each key for enabling communication between the client and a respective service from the set of available services and including all additional authentication information required by the respective service for authenticating the user to the respective service, thereby enabling the client to access the available services without storing the service communication code and keys at the client or having to carry or remember them.

[Please cancel claim 7.]

8. (Currently amended) The system of claim 6, wherein the security services use a digital signature to authenticate the user ~~client~~ to determine the [client] user privileges.

9. (Previously amended) The system of claim 6, wherein the host engine forwards to the client security code for enabling the client to perform a security protocol recognized by the security services.

10. (Currently amended) The system of claim 6, wherein one of the available services is secured by a firewall and one of the keys ~~is configured~~ includes the additional authentication information to enable communication through the firewall.

11. (Previously amended) The system of claim 6, further comprising a firewall for protecting the system.

12. (Previously amended) The system of claim 6, wherein one of the keys includes an address identifying the location of the selected service.

13. (Previously amended) The system of claim 6, wherein the code uses a key to provide to the client a direct connection with the selected service.

14. (Previously amended) The system of claim 6, further comprising a proxy for communicating with the selected service, and wherein the code enables the client to communicate with the proxy and one of the keys enables the proxy to locate the selected service.

16. (Previously amended) The method of claim 20, wherein establishing a communications link includes the step of using SSL to create a secure communications link with the client.

17. (Previously amended) The method of claim 20, wherein establishing a communications link includes the step of negotiating an encryption protocol for transferring messages to and from the client.

18. (Previously amended) The method of claim 20, wherein establishing a communications link includes the step of using public key certificates for transferring messages to and from the client.

19. (Currently amended) The method of claim 20, wherein determining user ~~client~~ privileges includes the step of using public key certificates to authenticate a user of the client.

20. (Currently amended) A computer-based method comprising:

establishing a communications link with a client;

presenting to a user of the client a plurality of user authentication protocol options, each user authentication protocol option having a particular level of authentication associated with it;

authenticating the user according to at least one user authentication protocol option;

determining user ~~client~~ privileges~~, the determining including the step of examining~~ based on the identity of a user ~~of the client~~ and the level of authentication;

presenting a set of available services based on the user privileges, at least one of the available services requiring additional authentication information to be provided before access to the service is granted;

enabling the client to select a particular service from a set of available ~~personal information management~~ services~~, the set of available services based on the client privileges~~;

providing to the client service communication code that enables communication with ~~a selected~~ the particular service; and

retrieving a key from a set of keys, each key corresponding to a respective service from the set of available services, the retrieved key for enabling communication between the client and the ~~selected~~ particular service and including all additional authentication information required by the respective service for authenticating the user to the respective service, thereby enabling the client to access the available services without storing the service communication code and keys at the client or having to carry or remember them.

Please cancel claim 21.

22. (Currently amended) The method of claim 20, wherein determining user ~~client~~ privileges includes the step of using a digital signature to authenticate the user ~~client~~.

23. (Previously amended) The method of claim 20, wherein establishing a communications link includes forwarding to the client security code for enabling the client to perform a recognized security protocol.

24. (Previously amended) The method of claim 20, further comprising the step of using one of the keys to communicate through a firewall to the selected service.

25. (Previously amended) The method of claim 20, wherein the method is performed by a server and further comprising using a firewall to protect the server.

26. (Previously amended) The method of claim 20, wherein one of the keys includes an address identifying the location of the selected service.

27. (Previously amended) The method of claim 20, wherein providing includes the step of providing to the client a direct connection with the service.

28. (Previously amended) The method of claim 20, further comprising using a proxy to communicate with the service, and wherein providing includes enabling the client to communicate with the proxy.

29. (Currently amended) A system on a server computer system, comprising:

means for establishing a communications link with a client;

means for presenting to a user of the client a plurality of user authentication protocol options, each user authentication protocol option having a particular level of authentication associated with it, for authenticating the user according to at least one user authentication protocol, and for determining ~~client~~ user privileges ~~including means for examining~~ based on the identity of a user ~~of the client~~ and the level of authentication;

means for presenting a set of available services based on the user privileges, at least on of the available services requiring additional authentication information to be provided before access to the service is granted, and for enabling the client to select a particular service from a set of available ~~personal information management~~ services~~, the set of available services based on the client privileges~~;

means for providing to the client service communication code that enables communication with ~~a selected~~ the particular service; and

means for retrieving a key from a set of keys, each key corresponding to a respective service from the set of available services, the retrieved key for enabling communication between the client and the ~~selected~~ particular service and including all additional authentication information required by the respective service for authenticating the user to the respective service, thereby enabling the client to access the available services without storing the service communication code and keys at the client.

30. (Currently amended) A computer-based storage medium storing a program for causing a computer to perform the steps of:

establishing a communications link with a client;

presenting to a user of the client a plurality of user authentication protocol options, each user authentication protocol option having a particular level of authentication associated with it;

authenticating the user according to at least one user authentication protocol option;

determining user ~~client~~ privileges~~, the determining including the step of examining~~ based on the identity of a user ~~of the client~~ and the level of authentication;

presenting a set of available services based on the user privileges, at least one of the available services requiring additional authentication information to be provided before access to the service is granted;

enabling the client to select a particular service from a set of available ~~personal information management~~ services~~, the set of available services based on the client privileges~~;

providing to the client service communication code that enables communication with ~~a selected~~ the particular service; and

retrieving a key from a set of keys, each key corresponding to a respective service from the set of available services, the retrieved key for enabling communication between the client and the ~~selected~~ particular service and including all additional authentication information required by the respective service for authenticating the user to the respective service, thereby enabling the client to access the available services without storing the service communication code and keys at the client or having to carry or remember them.

32. (Currently amended) A method, comprising:

receiving, from a client, as an advance communication, security information corresponding to one or more secured network ~~personal information management~~ services;

storing the security information at a location remote from the client;

receiving a client request from the client to access a secured network ~~personal information management~~ service; and

using the stored security information to enable the client access to the secured network service without requiring the client to supply the stored security information.

33. (Previously amended) A method according to claim 32, wherein the security information includes one or more keys corresponding to respective ones of the secured network services.

34. (Previously amended) A method according to claim 32, wherein at least one of the keys includes a certificate for accessing at least one of the secured network services.

~~#2~~
#1

35. (Previously amended) A method according to claim 32, further comprising determining client privileges of the client, and wherein the using the stored security information is provided if the privileges correspond to privilege requirements of the secured network service.

36. (Previously amended) A method according to claim 32, further comprising determining client privileges of the client and enabling the client to select a service from ones of the secured network services corresponding to the determined client privileges.

37. (Currently amended) A system, comprising:

means for receiving, from a client, as an advance communication, security information corresponding to one or more secured network ~~personal information management~~ services;

means for storing the security information at a location remote from the client;

means for receiving a client request from the client to access a secured network ~~personal information management~~ service; and means for using the stored security information to enable the client access to the secured network service without requiring the client to supply the stored security information.

38. (Currently amended) A computer-readable storage medium storing program code for causing a computer to perform the steps of:

receiving, from a client, as an advance communication, security information corresponding to one or more secured network ~~personal information management~~ services;

storing the security information at a location remote from the client;

receiving a client request from the client to access a secured network ~~personal information management~~ service; and

using the stored security information to enable the client access to the secured network service without requiring the client to supply the stored security information.

Please add the following new claim.

39. (Currently added) A server computer system, comprising:

a communications engine for establishing a communications link with a client;

security services coupled to the communications engine for presenting a user of the client a plurality of user authentication protocol options, each user authentication protocol option having a particular level of authentication associated with it, for authenticating the user according to at least one user authentication protocol and for determining user privileges based on the identity of the user and the level of authentication; and

a web server for presenting information to the user based on the user privileges.